(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 November 2001 (15.11.2001)

PCT

(10) International Publication Number
WO 01/86864 A2

(51) International Patent Classification[7]: H04L 12/00

(21) International Application Number: PCT/US01/13732

(22) International Filing Date: 27 April 2001 (27.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/202,190	5 May 2000 (05.05.2000)	US
09/588,634	6 June 2000 (06.06.2000)	US

(71) Applicant: **FUJITSU NETWORK COMMUNICATIONS, INC.** [US/US]; 2801 Telecom Parkway, Mail Station 2C, Richardson, TX 75082 (US).

(72) Inventors: **MO, Li**; 4585 Spencer Drive, Plano, TX 75024 (US). **WIDJAJA, Indra**; 265 Avalon Gardens Drive, Nanuet, NY 10954 (US). **SULLIVAN, Edward, T.**; 417 Moran Drive, Highland Village, TX 75067 (US). **WYNN, David, W.**; 2614 Big Oaks Drive, Garland, TX 75044 (US).

(74) Agent: **SHOWALTER, Barton, E.**; Baker Botts L.L.P., 2001 Ross Avenue, Dallas, TX 75201-2980 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/86864 A2

(54) Title: METHOD AND SYSTEM FOR PROVIDING A PROTECTION PATH FOR CONNECTION-ORIENTED SIGNALS IN A TELECOMMUNICATIONS NETWORK

(57) Abstract: A system is provided for providing a protection path for connection-oriented signals in a telecommunications network comprising a plurality of nodes. The system includes a source node, a destination node and a penultimate node. The source node is operable to transmit traffic. The destination node is operable to receive traffic from the source node. The penultimate node is operable to receive traffic from the source node, to transmit traffic directly to the destination node, to designate one of the nodes as a reflector and to generate a first segment of a protection path from the penultimate node through the reflector to the destination node.

METHOD AND SYSTEM FOR PROVIDING A PROTECTION PATH FOR CONNECTION-ORIENTED SIGNALS IN A TELECOMMUNICATIONS NETWORK

TECHNICAL FIELD OF THE INVENTION

This invention relates generally to the field of telecommunications and more particularly to a method and system for providing a protection path for connection-oriented signals in a telecommunications network.

BACKGROUND OF THE INVENTION

Telecommunications systems generally operate in either a connection-oriented mode or a connectionless mode. In a connection-oriented mode of operation, signals are communicated over specified paths from a source network element to a destination network element. Connection-oriented signals include, for example, Multi-Protocol Label Switching signals with Asynchronous Transport Mode (ATM), frame relay, or packet-over-SONET encoding.

When a failure occurs along the specified working path in connection-oriented communication, the signals must be re-routed to the destination network element along another available path. Previous attempts to provide for the delivery of connection-oriented signals via an alternate route have included global repair, per-area repair and local repair.

For global repair, the node closest to the failure generates failure notification messages that are delivered to the source network element. The source network element then switches the signals to a protection path. Bandwidth is reserved on the protection path in an amount equal to the working path bandwidth.

Using a global repair scheme, however, may result in time limits for recovery being unmet due to long distances between the point of failure and the source network element. In addition, the node detecting the failure needs a way to send a reliable failure notification message to each source network element that is affected by the failure. Also, the failure notification message must be understood by the source network element. However, using global repair across different routing areas may prevent the source network elements from understanding the failure notification messages. Using global repair also results in the reservation of protection path bandwidth that prevents other traffic sources from using an optimal path, thereby reducing the total network efficiency.

For per-area repair, protection switching is isolated to a single area of network elements. However, this type of repair wastes bandwidth and results in an increased number of paths that must be maintained. In addition, per-area repair requires the use of two border nodes at every border between two different areas.

For local repair, protection switching is initiated by a node adjacent to the failure. Thus, for example, local repair schemes may include deflective routing. However, the use of local repair fails to provide for bandwidth reservation for general topologies to guarantee bandwidth for protected traffic.

SUMMARY OF THE INVENTION

In accordance with the present invention, a method and system for providing a protection path for connection-oriented signals in a telecommunications network are provided that substantially eliminate or reduce disadvantages and problems associated with previously

developed systems and methods. In particular, reflectors are used to provide a plurality of segments for a protection path, thereby reducing overall packet delay and satisfying Quality of Service requirements.

In one embodiment of the present invention, a system is provided for providing a protection path for connection-oriented signals in a telecommunications network comprising a plurality of nodes. The system includes a source node, a destination node and a penultimate node. The source node is operable to transmit traffic. The destination node is operable to receive traffic from the source node. The penultimate node is operable to receive traffic from the source node, to transmit traffic directly to the destination node, to designate one of the nodes as a reflector and to generate a first segment of a protection path from the penultimate node through the reflector to the destination node.

In another embodiment of the present invention, a node is provided in a telecommunications network. The node includes an ingress port, a reflector identifier, a protection path generator, and an egress port. The ingress port is operable to receive traffic. The traffic comprises a working path, a protection path, working traffic and protection traffic. The reflector identifier is operable to identify the node as a reflector based on the received traffic. The protection path generator is operable to generate a protection path based on an identification of the node as a reflector. The egress port is operable to transmit traffic.

Technical advantages of the present invention include providing an improved method for providing a protection path for connection-oriented signals in a telecommunications network. In particular, a penultimate

node in the working path designates a reflector and generates a segment of a protection path from the penultimate node through the reflector to the destination node. The reflector then generates another segment of the protection path. Accordingly, the protection path comprises a plurality of segments each operable to provide protection for a distinct protection domain. As a result, protection capability and flexibility is increased, protection switching delays are decreased, and network efficiency is improved.

Other technical advantages of the present invention include providing a method for generating a protection path for a packet-switched network. In particular, a plurality of segments making up a protection path are generated by nodes in the working path. As a result, a protection path is provided for a packet-switched network without the need for each node detecting a failure to generate failure notification messages for the source network element. In addition, network elements need not be partitioned into different protection areas.

Other technical advantages will be readily apparent to one skilled in the art from the following figures, description, and claims.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention and its advantages, reference is now made to the following description taken in conjunction with the accompanying drawings, wherein like numerals represent like parts, in which:

FIGURE 1 is a block diagram illustrating a communication system operable to facilitate communication

of connection-oriented signals in accordance with one embodiment of the present invention;

FIGURE 2 is a block diagram illustrating a system for providing a protection path for connection-oriented signals communicated between the nodes of FIGURE 1 in accordance with one embodiment of the present invention;

FIGURE 3 is a block diagram illustrating one of the nodes of FIGURE 2 operable to provide a protection path for connection-oriented signals in accordance with one embodiment of the present invention;

FIGURE 4 is a flow diagram illustrating a method for providing a protection path for connection-oriented signals communicated between the nodes of FIGURE 1 in accordance with one embodiment of the present invention; and

FIGURE 5 is a flow diagram illustrating a method for reserving bandwidth for connection-oriented signals communicated between the nodes of FIGURE 1 in accordance with one embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

FIGURE 1 is a block diagram illustrating a communication system 10 operable to facilitate communication of connection-oriented signals in accordance with one embodiment of the present invention. The telecommunications network is a network that transmits voice, audio, video or other suitable types of information, and/or a combination of different types of information between source and destination points. As used herein, the term "connection-oriented signal" refers to any signal associated with a particular path, or portion of a path, from a source network element to a destination network element. For example, connection-oriented signals include

Multi-Protocol Label Switching (MPLS) signals with ATM, frame relay or packet-over-SONET encoding.

The system 10 is operable to provide either connection-oriented communication or a hybrid of connectionless and connection-oriented communication, as described in the co-owned U.S. Patent Application entitled, "System and Method for Connectionless/Connection Oriented Signal Transport," filed on June 6, 2000. The system 10 comprises a core cloud 12 that comprises one or more core network elements 14, or nodes 14. The nodes 14 may communicate with each other via communication links 16 and with one or more peripheral network elements 20 via communication links 30. The communication links 16 and 30 may comprise any wireless, wireline, fiber or other communication medium or combinations of media. A signal communicated via communication links 16 and/or 30 may comprise an electrical signal, an optical signal, or any other suitable type of signal or combination of signals.

The peripheral network elements 20 facilitate communication between the core cloud 12 and other network elements coupled to other networks, such as networks 36. According to the illustrated embodiment, the peripheral network elements 20 comprise routers 20. Each router 20 couples the core cloud 12 to a network 36 via a communication link 50. As used herein, "each" means every one of at least a subset of the identified items.

The routers 20 facilitate routing functions for signals originated or forwarded by interface equipment 40 and communicated over the networks 36. The interface units 40 comprise personal computers, servers, switches, routers or any other suitable network equipment operable to originate or forward communication signals. In accordance with one embodiment, the interface units 40 operate to

communicate MPLS signals with ATM, frame relay and/or packet-over-SONET encoding or any other suitable label-switched signals. It will be understood, however, that interface units 40 communicating other types of signals may be coupled to the networks 36 without departing from the scope of the present invention.

The networks 36 may comprise any suitable wireline or wireless systems that support communication between network elements using ground-based and/or space-based components. For example, the networks 36 may comprise public switched telephone networks, integrated services digital networks, local area networks, wide area networks, or any other suitable communication systems or combination of communications systems at one or more locations. Each of the networks 36 may comprise a single network or multiple networks.

In operation, the core cloud 12 receives connection-oriented signals from the peripheral network elements 20 and routes those signals through the core cloud 12 to another appropriate peripheral network element 20 according to routing rules associated with the received signal. In a particular embodiment, an ingress node 14 receives an incoming signal from a peripheral network element 20 and appends a transport label to the incoming signal which contains instructions or an index to instructions to other nodes 14 on how to process the signal.

The ingress node 14 identifies an egress node 14 associated with a destination peripheral network element 20 and communicates the signal toward the egress node 14. The nodes 14 residing between the ingress node and the egress node 14 receive the signal with the appended transport label and process the signal in accordance with the transport label.

FIGURE 2 is a block diagram illustrating a system 60 for providing a protection path for connection-oriented signals communicated between the nodes 14 in accordance with one embodiment of the present invention. According to one embodiment, a protection path comprises reserved bandwidth that is available for protection traffic. The system 60 comprises a plurality of nodes 14, including a source node 62 for transmitting traffic to a destination node 64 along a working path 66 that comprises a plurality of other nodes 14. In the illustrated embodiment, the nodes 14 are numerically labeled 1-8 for discussion purposes; however, it will be understood that any suitable number of nodes 14 may exist along the working path 66 between the source node 62 and the destination node 64. Thus, each node 14 may represent 0, 1 or more nodes 14.

The system 60 also comprises a penultimate node 68, which is the node 14 that is operable to transmit working traffic along the working path 66 directly to the destination node 64. As used herein, "directly" refers to communication from one node 14 to another node 14 with no intervening nodes 14 between them. Similarly, as used herein, "indirectly" refers to communication from one node 14 to another node 14 through one or more intervening nodes 14. In addition, two nodes 14 are coupled to each other when the nodes 14 are operable to communicate with each other either directly or indirectly. Once the working path 66 is established from the source node 62 to the destination node 64, the penultimate node 68 is operable to identify itself as the penultimate node 68 and to establish a protection domain 70a by generating a first segment 72a of a protection path 72.

The system 60 comprises a plurality of protection domains 70, each of which comprises a reflector 74 and one

or more inner nodes 14. A reflector 74 comprises a node 14 that is operable to transmit protection traffic to a node 14 that is outside and downstream of the protection domain 70 comprising that reflector 74. Each reflector 74 may transmit protection traffic to the downstream node 14 either directly or indirectly; however, any intervening nodes 14 may not be within the protection domain 70 comprising the reflector 74. The inner nodes 14 are nodes 14 other than reflectors 74 and the destination node 64. Thus, in the illustrated embodiment, nodes one, two, four, five, seven and eight are inner nodes 14.

Each segment 72a, b or c of the protection path 72 begins at the most downstream node 14 in the corresponding protection domain 70a, b or c, continues upstream through the inner nodes 14 until arriving at the reflector 74, and ends at another node 14 outside and downstream of the protection domain 70a, b or c. Thus, each protection domain 70, other than the protection domain 70 comprising the source node 62, may receive working traffic from an upstream protection domain 70 through its own reflector 74 and may receive protection traffic from the reflector 74 for the upstream protection domain 70 through one of its own inner nodes 14.

As used herein, "upstream" refers to a node 14 that is closer to the source node 62 than the reference node 14. Similarly, as used herein, "downstream" refers to a node 14 that is closer to the destination node 64 than the reference node 14. In addition, although the illustrated embodiment comprises three protection domains 70a, b and c, it will be understood that the present invention may be implemented with any suitable number of protection domains 70.

The penultimate node 68 designates a node 14 as a reflector 74 for the first protection domain 70a and generates the first segment 72a of the protection path 72 by providing an order of nodes 14 corresponding to the path for protection traffic within the first protection domain 70a to each of those nodes 14. Thus, for the illustrated embodiment, the first segment 72a comprises node eight, followed by node seven, followed by node six and finally the destination node 64. This order of nodes 14 is provided by the penultimate node 68 to the ordered nodes 14.

A node 14 is designated as a reflector 74 based on distance, propagation delay, or any other suitable criteria, such that the overall delay due to a failure in a node 14 or a link between the nodes 14 is kept below a pre-defined time limit. In addition, a node 14 is designated as a reflector 74 based on Quality of Service considerations for the traffic.

Node six, which is the reflector 74 for the first protection domain 70a, identifies itself as a reflector 74 based on the first segment 72a provided to node six. Because the node 14 that is subsequent to node six in the path for protection traffic corresponding to the first segment 72a is also downstream of node six, node six recognizes itself as a reflector 74. In contrast, for example, the node 14 that is subsequent to node seven in the first segment 72a is upstream of node seven. Thus, node seven recognizes that it is not a reflector 74.

In an alternative embodiment, node six may recognize itself as a reflector 74 by recognizing that the node 14 subsequent to node six in the protection path 72 is not a node 14 from which node six directly receives working traffic. For this embodiment, node seven recognizes that

it is not a reflector 74 by recognizing that the node 14 subsequent to node seven in the protection path 72 is a node 14 from which node seven directly receives working traffic.

After recognizing itself as a reflector, node six is operable to generate a second segment 72b of the protection path 72 in a similar manner to the generation of the first segment 72a by the penultimate node 68. Node six identifies an upstream node 14 adjacent to node six. In the illustrated embodiment, this upstream node 14 is node five. Node six also identifies a downstream node 14 that is adjacent to node six. In the illustrated embodiment, this downstream node 14 is node seven. As a reflector 74, node six also designates a node 14 that is upstream of itself as a next reflector 74. In the illustrated embodiment, this next reflector 74 is node three.

For this embodiment, node six generates the second segment 72b of the protection path 72 by providing an order of nodes 14 corresponding to the path for protection traffic within the second protection domain 70b to each of those nodes 14. Thus, for the illustrated embodiment, the second segment 72b comprises node five, followed by node four, followed by node three and finally node seven. This order of nodes 14 is provided by the reflector 74, or node six, to the ordered nodes 14. Thus, the second segment 72b of the protection path 72 allows protection traffic to be routed from the second protection domain 70b to the first protection domain 70a when the working path 66 is unavailable at any point between node three and node six.

Similar to node six, node three as a reflector 74 generates a third segment 72c of the protection path 72 from node two, to node one, to the source node 62 and finally to node four. Thus, a complete protection path 72

is provided in a plurality of segments 72a, b and c, each of which corresponds to a protection domain 70a, b or c.

FIGURE 3 is a block diagram illustrating one of the nodes 14 operable to provide a protection path 72 for connection-oriented signals in accordance with one embodiment of the present invention. The node 14 comprises one or more ingress ports 100 and 102 for receiving traffic, one or more egress ports 104 and 106 for transmitting traffic, a penultimate node identifier 120 for identifying the node 14 as a penultimate node 68, a reflector identifier 122 for identifying the node 14 as a reflector 74, a protection path generator 124 for generating a segment 72a, b or c of a protection path 72, and a traffic classifier 126 for classifying traffic received through an ingress port 100 or 102 as working traffic or protection traffic.

According to the illustrated embodiment, the ingress ports comprise a working ingress port 100 for receiving working traffic on the working path 66 and a protection ingress port 102 for receiving protection traffic on the protection path 72. Similarly, the egress ports comprise a working egress port 104 for transmitting working traffic on the working path 66 and a protection egress port 106 for transmitting protection traffic on the protection path 72. However, it will be understood that the node 14 may comprise one or more ingress ports 100 and 102, each of which may receive working and/or protection traffic. In addition, the node 14 may comprise one or more egress ports 104 and 106, each of which may transmit working and/or protection traffic.

The penultimate node identifier 120 is operable to identify the node 14 as a penultimate node 68 based on the working path 66 which indicates that the node 14 is

operable to transmit working traffic directly to the destination node 64 along the working path 66. Thus, if the node 14 is operable to transmit working traffic directly to the destination node 64, the penultimate node identifier 120 notifies the node 14 of its status as the penultimate node 68. Otherwise, the node 14 recognizes that it is not the penultimate node 68.

The reflector identifier 122 is operable to identify the node 14 as a reflector 74 based on the protection path 72. Each node 14 in a segment 72a, b or c of a protection path 72 transmits protection traffic to a node 14 upstream of itself, except for a reflector 74 which transmits protection traffic downstream of itself to a node 14 in another protection domain 70. Thus, the reflector identifier 122 is operable to recognize that the node 14 in the protection path 72 subsequent to the node 14 comprising the reflector identifier 122 is downstream of that node 14. In this situation, the reflector identifier 122 notifies the node 14 of its status as a reflector 74. Otherwise, the node 14 recognizes that it is not a reflector 74.

The protection path generator 124 is operable to generate a segment 72a, b or c of a protection path 72. If the penultimate node identifier 120 has identified the node 14 as the penultimate node 68 or if the reflector identifier 122 has identified the node 14 as a reflector 74, the protection path generator 124 generates a segment 72a, b or c of the protection path 72, as described in more detail above in connection with FIGURE 2.

The traffic classifier 126 is operable to classify traffic received at the node 14 as either working traffic or protection traffic. According to the illustrated embodiment, the traffic classifier 126 may classify traffic received at the working ingress port 100 as working traffic

and traffic received at the protection ingress port 102 as protection traffic. In an alternative embodiment, both working and protection traffic may be received at a same ingress port 100 or 102. For this embodiment, the traffic may comprise a traffic identifier identifying itself as either working traffic or protection traffic. The traffic classifier 126 is then operable to classify the received traffic based on the traffic identifier for the traffic. It will be understood that the traffic classifier 126 may classify the traffic as working or protection traffic in any other suitable manner without departing from the scope of the present invention. Based on the classification of the traffic by the traffic classifier 126, the node 14 routes the working traffic along the working path 66 and protection traffic along the protection path 72.

FIGURE 4 is a flow diagram illustrating a method for providing a protection path 72 for connection-oriented signals communicated between the nodes 14 in accordance with one embodiment of the present invention. The method begins at step 400 where a working path 66 is established from a source node 62 to a destination node 64.

At step 402, the penultimate node identifier 120 for the node 14 that transmits working traffic directly to the destination node 64 identifies the node 14 as the penultimate node 68. At step 404, the penultimate node 68 designates a node 14 as a reflector 74. At step 406, the penultimate node 68 generates a first segment 72a of a protection path 72 from the penultimate node 68 through the reflector 74 to the destination node 64.

At decisional step 408, a determination is made regarding whether the reflector 74 is the source node 62. If the reflector 74 is the source node 62, the entire protection path 72 has been generated and the method

follows the Yes branch from decisional step 408 where it comes to an end. However, if the reflector 74 is not the source node 62, the method follows the No branch from decisional step 408 to step 410.

At step 410, the reflector 74 identifies the upstream node 14 adjacent to the reflector 74. At step 412, the reflector 74 identifies the downstream node 14 adjacent to the reflector 74. At step 414, the reflector 74 designates a node 14 as a next reflector 74. At step 416, the reflector 74 generates a second segment 72b of the protection path 72 from the upstream node 14 through the next reflector 74 to the downstream node 14.

At decisional step 418, a determination is made regarding whether the next reflector 74 is the source node 62. If the next reflector 74 is the source node 62, the entire protection path 72 has been generated and the method follows the Yes branch from decisional step 418 where it comes to an end. However, if the next reflector 74 is not the source node 62, the method follows the No branch from decisional step 418 and returns to step 410 to generate another segment of the protection path 72. Thus, the method continues until a next reflector 74 is the source node 62, indicating that the entire protection path 72 has been generated. In this way, a protection path 72 is provided that comprises a plurality of segments 72a, b and c such that processing delays and the amount of failure notification messages generated are substantially reduced, resulting in more timely and efficient communication of the signals. In addition, the protection path 72 is generated as a result of the working path 66 being established such that the protection path 72 is readily available should a failure occur, thereby reducing delays in responding to a failure.

FIGURE 5 is a flow diagram illustrating a method for reserving bandwidth for connection-oriented signals communicated between the nodes 14 in accordance with one embodiment of the present invention. The method begins at step 500 where a working bandwidth for a central node is reserved. A central node comprises any node 14 operable to receive traffic from a plurality of peripheral nodes.

At step 502, working bandwidth is determined for the central node based on the amount of working traffic that may be received from a particular peripheral node, assuming that the corresponding working path 66 is available. At step 504, protection bandwidth is determined for the central node based on the amount of protection traffic that may be received from the peripheral node, assuming that the corresponding working path 66 is unavailable.

At step 506, the working bandwidth for the central node based on the working traffic from the peripheral node is compared to the protection bandwidth for the central node based on the protection traffic from the peripheral node. At decisional step 508, a determination is made regarding whether the protection bandwidth is greater than the working bandwidth. If the protection bandwidth is greater than the working bandwidth, the method follows the Yes branch from decisional step 508 to step 510. At step 510, additional working bandwidth is reserved for the central node in accordance with the difference between the protection bandwidth and the working bandwidth associated with the peripheral node.

Returning to decisional step 508, if the protection bandwidth is not greater than the working bandwidth, the method follows the No branch from decisional step 508 to step 512. At step 512, no additional working bandwidth is reserved for the central node based on the peripheral node.

From steps 510 and 512, the method continues to decisional step 514. At decisional step 514, a determination is made regarding whether there are more peripheral nodes that may contribute to the bandwidth requirement for the central node. If there are more peripheral nodes, the method follows the Yes branch from decisional step 514 and returns to step 502 in order to determine whether or not to reserve additional bandwidth for another peripheral node. However, if there are no more peripheral nodes, the method follows the No branch from decisional step 514 and comes to an end. In this way, bandwidth is reserved for the central node in accordance with the bandwidth requirements contributed by each of the peripheral nodes from which the central node receives traffic.

According to one embodiment, bandwidth is reserved for the protection path 72 to provide protection based on Quality of Service. The following notations are introduced to facilitate the discussion of this embodiment.

The set of all nodes 14 in the telecommunications network will be denoted as N_T. Each node 14 can be expressed as I_x where x is the index of the set N_T. The count of this set is $C(N_T)$.

The set of all unidirectional links in the telecommunications network will be denoted as L_T. Each member of L_T will be represented as l_i, with i being the index of the set L_T. The count of this set is $C(L_T)$.

Bandwidth reservation involves a determination of the required link bandwidth for protection purposes, expressed as P_{l_x} for any link l_x inside the network. In determining protection bandwidth reservation for a link l_x, traffic from

other links and nodes 14 onto link l_x are considered, as discussed below.

For any working link l_y inside the network that sends working traffic onto link l_x, the bandwidth for this portion of the traffic on link l_x is expressed as $B_w(l_y/l_x)$ (bandwidth of the working traffic from l_y to l_x). If link l_y is broken, such traffic disappears.

For any broken link l_y inside the network, bandwidth for the protection traffic directed onto link l_x due to the broken status of link l_y is expressed as $B_p(l_y/l_x)$.

For any working node I_y inside the network that sends working traffic onto link l_x, the bandwidth for this portion of the traffic on link l_x is expressed as $B_w(I_y/l_x)$ (bandwidth of the working traffic from node I_y to l_x). If node I_y is broken, such traffic disappears.

For any broken node I_y inside the network, bandwidth for the protection traffic directed onto link l_x due to the broken status of node I_y is expressed as $B_p(I_y/l_x)$.

Thus, for protecting against a failure on link l_y, the protection bandwidth on link l_x, expressed as $P_{lx}(l_y)$, is given by:

$$P_{lx}(l_y) = \max(0, B_p(l_y/l_x) - B_w(l_y/l_x)) \qquad (eqn.\ 1)$$

Similarly, for protecting against a failure on node I_y, the protection bandwidth on link l_x, expressed as $P_{lx}(I_y)$, is given by:

$$P_{l_x}(I_y)=\max(0,B_p(I_y/l_x)-B_w(I_y/l_x)) \qquad (eqn.2)$$

Thus, an array can be established by considering each link and node 14 inside the network as follows:

$$[P_{l_x}(l_1),...,P_{l_x}(l_{C(L_T)}),P_{l_x}(I_1),...,P_{l_x}(I_{C(N_T)})] \qquad (eqn.3)$$

The array expressed in equation 3 can be numerically sorted and expressed as $\{p_1,p_2,...,p_n\}$ with $p_1 \geq p_2 \geq ... \geq p_n$ and $n=C(L_T)+C(N_T)$. For a single failure inside the network, the amount of bandwidth required for protection purposes is:

$$P_{l_x}=p_1 \qquad (eqn.4)$$

For M failures, the amount of the bandwidth required for protection purposes is:

$$P_{l_x}=(\sum_{j=1}^{M} p_j) \qquad (eqn.5)$$

Based on equation 3, it is also possible to specify a set of multiple failures for protection, depending on the protection policy (based on the importance of protecting certain links over others). Thus, this reservation mechanism minimizes the amount of bandwidth to be reserved for protection purposes.

Although the present invention has been described with several embodiments, various changes and modifications may be suggested to one skilled in the art. It is intended that the present invention encompasses such changes and

modifications as fall within the scope of the appended claims.

WHAT IS CLAIMED IS:

1. A system for providing a protection path for connection-oriented signals in a telecommunications network comprising a plurality of nodes, the system comprising:

a source node operable to transmit traffic;

a destination node operable to receive traffic from the source node; and

a penultimate node operable to receive traffic from the source node, to transmit traffic directly to the destination node, to designate one of the nodes as a reflector and to generate a first segment of a protection path from the penultimate node through the reflector to the destination node.

2. The system of Claim 1, the reflector operable to receive traffic, to identify the traffic as working traffic or protection traffic, to transmit the working traffic to a node downstream of the reflector and to transmit the protection traffic to the destination node.

3. The system of Claim 2, the reflector further operable to transmit the protection traffic directly to the destination node.

4. The system of Claim 2, the reflector further operable to designate one of the nodes as a next reflector and to generate a second segment of the protection path from a node upstream of the reflector through the next reflector to a node downstream of the reflector.

5. The system of Claim 4, the next reflector operable to receive traffic, to identify the traffic as working traffic or protection traffic, to transmit the

working traffic to a node downstream of the next reflector and to transmit the protection traffic to the node downstream of the reflector.

6. The system of Claim 5, the reflector further operable to transmit the protection traffic directly to the destination node, and the next reflector further operable to transmit the protection traffic directly to the node downstream of the reflector.

7. The system of Claim 4, the source node comprising the next reflector.

8. The system of Claim 1, the plurality of nodes comprising a plurality of inner nodes operable to transmit traffic between the source node and the reflector and between the reflector and the destination node, each of the inner nodes operable to receive traffic, to identify the traffic as working traffic or protection traffic, to transmit the working traffic to a node downstream of the inner node, and to transmit the protection traffic to a node upstream of the inner node.

9. The system of Claim 1, the source node comprising the reflector.

10. The system of Claim 1, the penultimate node further operable to designate one of the nodes as a reflector based on Quality of Service for the traffic.

11. A node in a telecommunications network, comprising:

an ingress port operable to receive traffic, the traffic comprising a working path, a protection path, working traffic and protection traffic;

a reflector identifier operable to identify the node as a reflector based on the received traffic;

a protection path generator operable to generate a protection path based on an identification of the node as a reflector; and

an egress port operable to transmit traffic.

12. The node of Claim 11, further comprising a traffic classifier operable to classify received traffic as working traffic or protection traffic.

13. The node of Claim 12, the traffic comprising a traffic identifier, the traffic classifier further operable to classify received traffic as working traffic or protection traffic based on the traffic identifier for the traffic.

14. The node of Claim 12, the egress port further operable to transmit working traffic based on the received working path and to transmit protection traffic based on the received protection path.

15. The node of Claim 12, the ingress port comprising a plurality of ports and the egress port comprising a plurality of ports.

16. The node of Claim 15, the ingress port comprising a working ingress port and a protection ingress port and

the egress port comprising a working egress port and a protection egress port, the traffic classifier further operable to identify traffic received through the working ingress port as working traffic and traffic received through the protection ingress port as protection traffic, the working egress port operable to transmit working traffic and the protection egress port operable to transmit protection traffic.

17. The node of Claim 12, further comprising a penultimate node identifier operable to identify the node as a penultimate node based on the received traffic, the protection path generator further operable to generate a protection path based on an identification of the node as a penultimate node.

18. The node of Claim 17, the node coupled to a destination node, the penultimate node identifier operable to identify the node as a penultimate node based on a determination that the node is operable to transmit working traffic directly to the destination node.

19. The node of Claim 11, the node coupled to a plurality of nodes, the reflector identifier operable to identify the node as a reflector based on the received protection path comprising a node downstream of the node subsequent to the node.

20. The node of Claim 11, the reflector identifier further operable to identify the node as a reflector based on Quality of Service for the traffic.

21. A method for providing a protection path for connection-oriented signals in a telecommunications network comprising a plurality of nodes, the method comprising:

identifying a source node operable to transmit traffic;

identifying a destination node operable to receive traffic from the source node;

identifying a penultimate node operable to transmit traffic directly to the destination node;

designating one of the nodes as a reflector; and

generating a first segment of a protection path from the penultimate node through the reflector to the destination node.

22. The method of Claim 21, further comprising:

identifying the traffic received at the penultimate node as working traffic or protection traffic;

transmitting the working traffic received at the penultimate node directly from the penultimate node to the destination node;

identifying the traffic received at the reflector as working traffic or protection traffic; and

transmitting the protection traffic received at the reflector directly from the reflector to the destination node.

23. The method of Claim 21, the source node comprising the reflector.

24. The method of Claim 21, further comprising:

designating one of the nodes as a next reflector; and

generating a second segment of the protection path from a node upstream of the reflector through the next reflector to a node downstream of the reflector.

25. The method of Claim 24, further comprising:

identifying the traffic received at the penultimate node as working traffic or protection traffic;

transmitting the working traffic received at the penultimate node directly from the penultimate node to the destination node;

identifying the traffic received at the reflector as working traffic or protection traffic;

transmitting the protection traffic received at the reflector directly from the reflector to the destination node;

identifying the traffic received at the next reflector as working traffic or protection traffic; and

transmitting the protection traffic received at the next reflector directly from the next reflector to the node downstream of the reflector.

26. The method of Claim 24, the source node comprising the next reflector.

27. The method of Claim 24, designating one of the nodes as a reflector comprising designating one of the nodes as a reflector based on Quality of Service for the traffic.

28. A method for reserving bandwidth for connection-oriented signals processed by a central node in a telecommunications network comprising a plurality of nodes, the method comprising:

identifying a plurality of peripheral nodes from which the central node receives traffic;

for each of the peripheral nodes, determining a working bandwidth for the central node based on working traffic from the peripheral node;

for each of the peripheral nodes, determining a protection bandwidth for the central node based on protection traffic from the peripheral node; and

for each of the peripheral nodes, reserving additional bandwidth for the central node when the protection bandwidth for the central node based on the peripheral node is greater than the working bandwidth for the central node based on the peripheral node.

29. The method of Claim 28, further comprising, for each of the peripheral nodes, reserving no additional bandwidth for the central node when the protection bandwidth for the central node based on the peripheral node is less than or equal to the working bandwidth for the central node based on the peripheral node.

30. The method of Claim 28, reserving additional bandwidth for the central node comprising reserving an additional amount of bandwidth corresponding to the difference between the protection bandwidth for the central node based on the peripheral node and the working bandwidth for the central node based on the peripheral node.

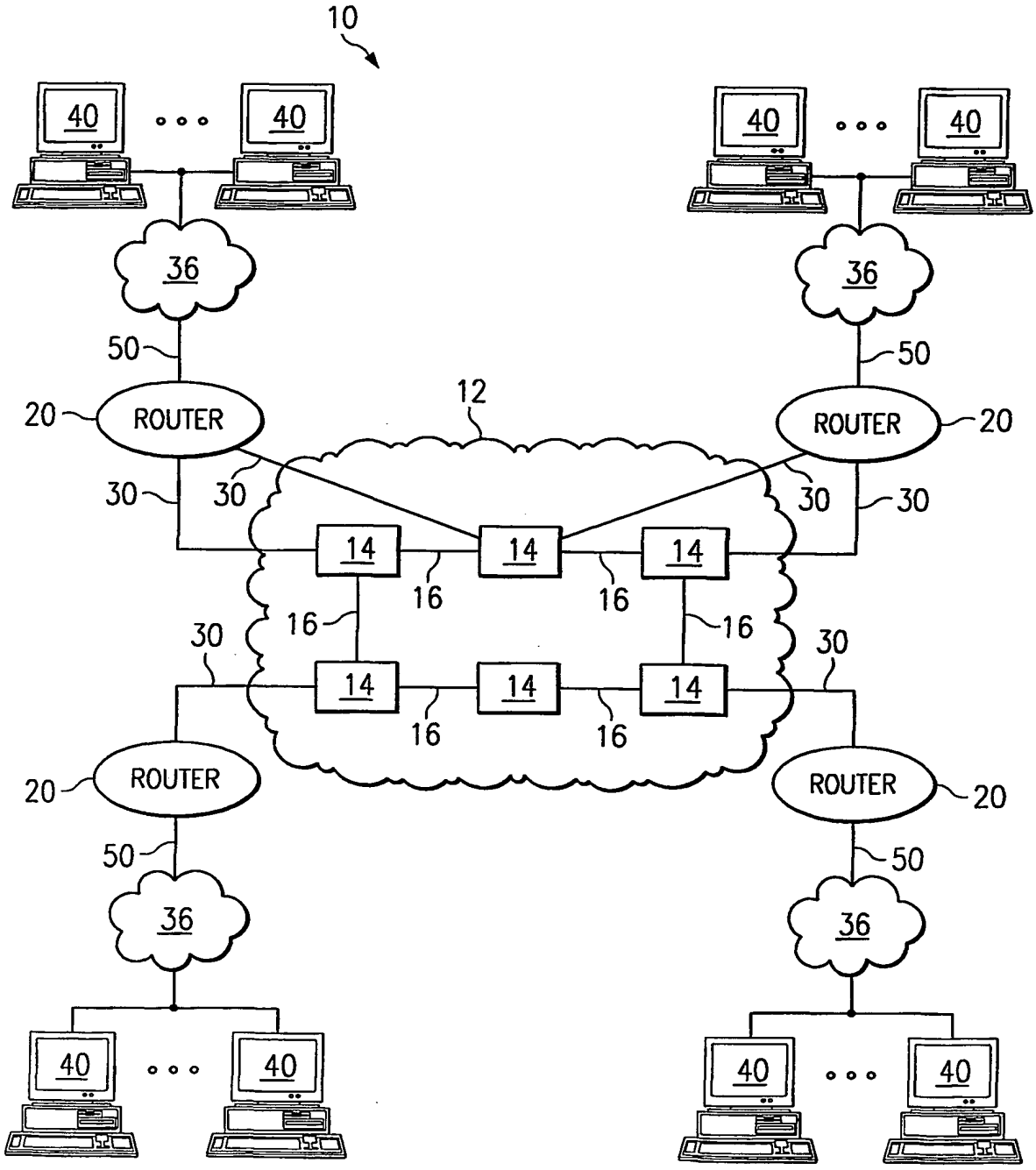

10
40
40
40
40
36
36
50
50
20
ROUTER
12
ROUTER
20
30
30
30
30
14
14
14
16
16
16
16
30
30
14
14
14
16
16
20
ROUTER
ROUTER
20
50
50
36
36
40
40
40
40

FIG. 1

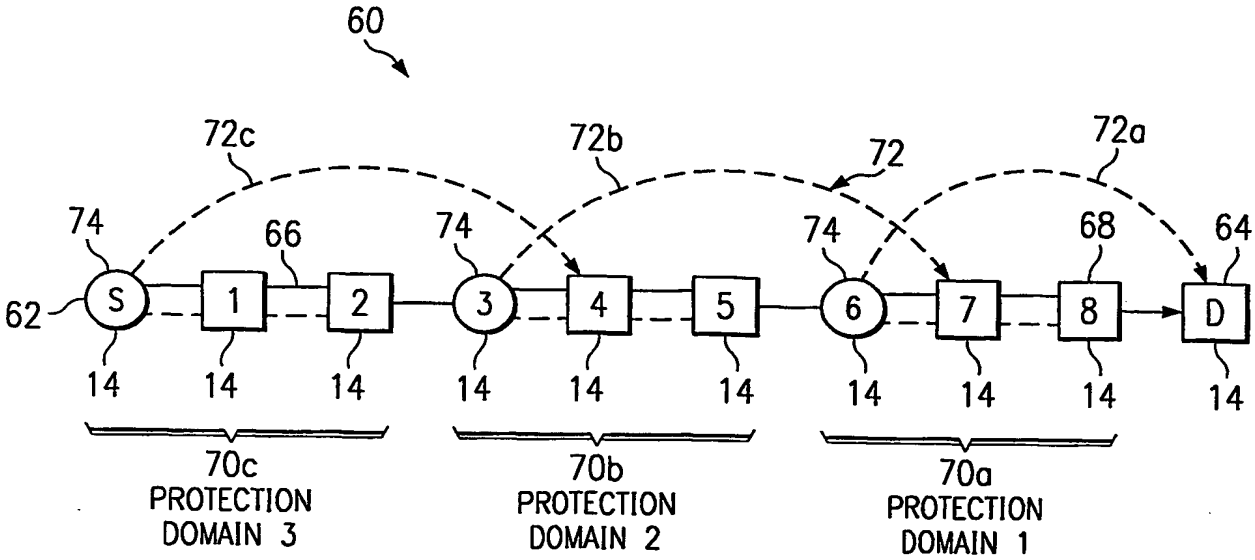

60
72c
72b
72
72a
74
66
74
74
68
64
62
S
1
2
3
4
5
6
7
8
D
14
14
14
14
14
14
14
14
14
14
70c
PROTECTION
DOMAIN 3
70b
PROTECTION
DOMAIN 2
70a
PROTECTION
DOMAIN 1

FIG. 2

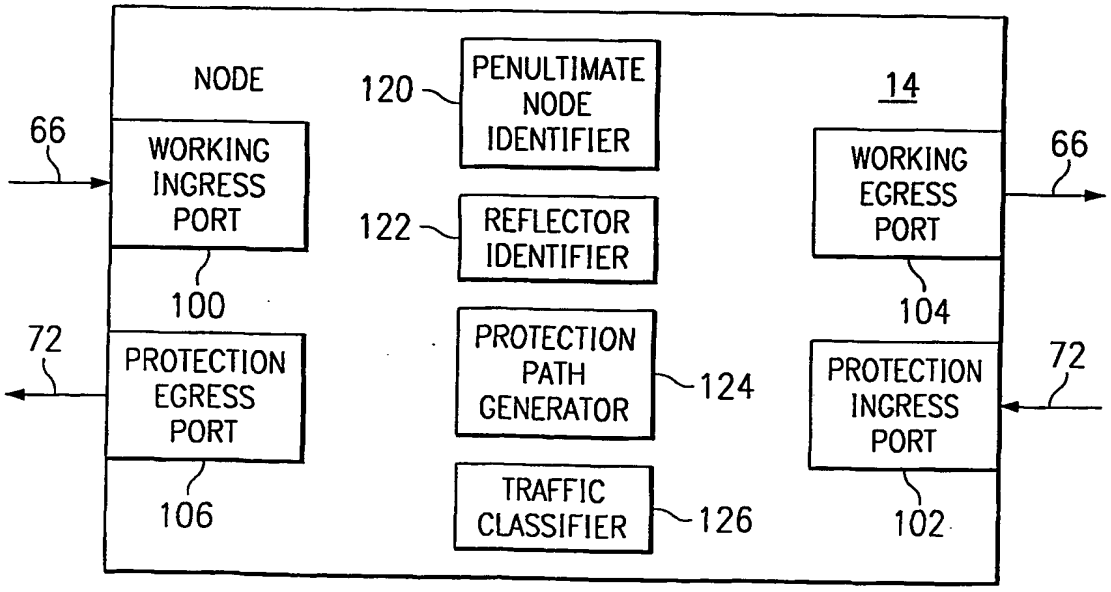

NODE
66
WORKING
INGRESS
PORT
100
72
PROTECTION
EGRESS
PORT
106
120
PENULTIMATE
NODE
IDENTIFIER
122
REFLECTOR
IDENTIFIER
PROTECTION
PATH
GENERATOR
124
TRAFFIC
CLASSIFIER
126
14
WORKING
EGRESS
PORT
66
104
PROTECTION
INGRESS
PORT
72
102

FIG. 3

FIG. 4

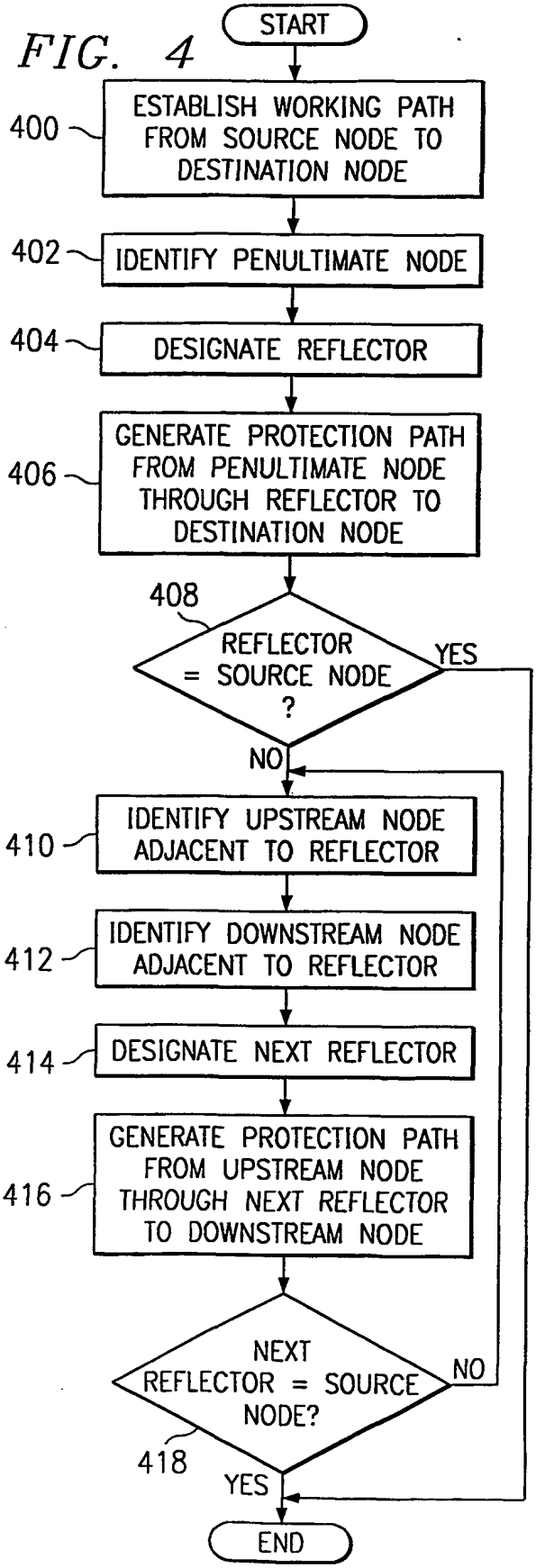
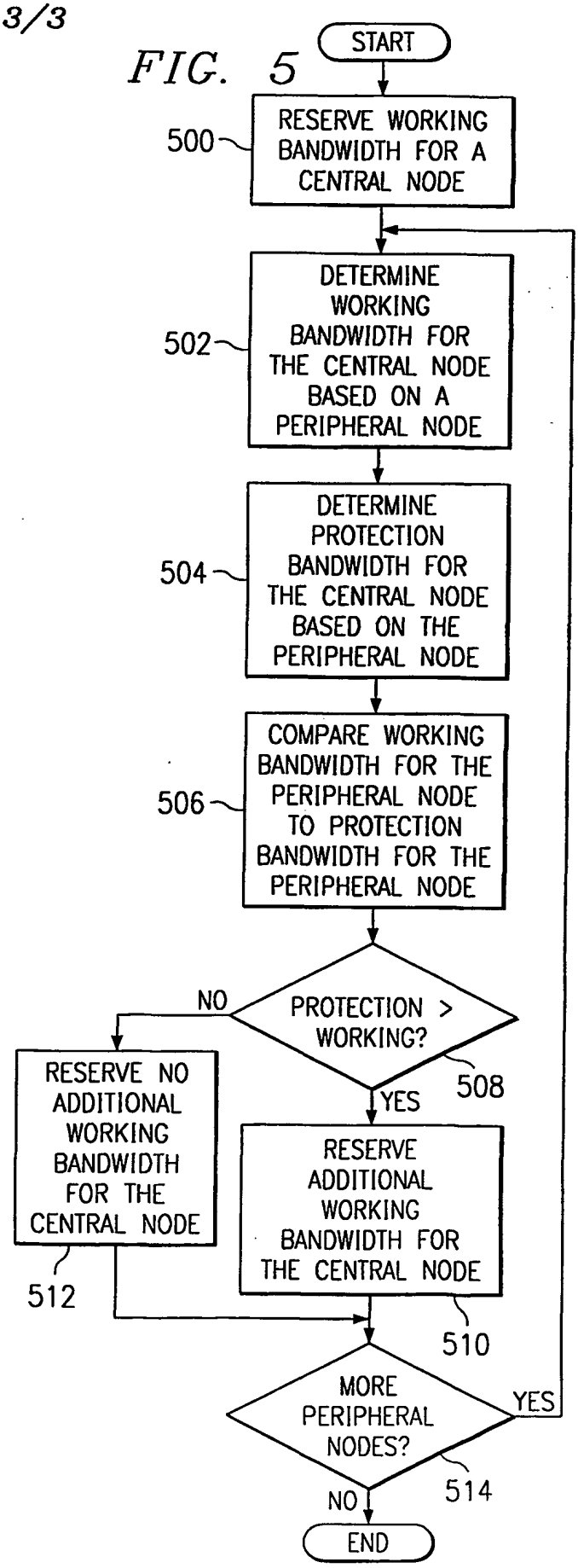

START
400
ESTABLISH WORKING PATH FROM SOURCE NODE TO DESTINATION NODE
402
IDENTIFY PENULTIMATE NODE
404
DESIGNATE REFLECTOR
406
GENERATE PROTECTION PATH FROM PENULTIMATE NODE THROUGH REFLECTOR TO DESTINATION NODE
408
REFLECTOR = SOURCE NODE ?
YES
NO
410
IDENTIFY UPSTREAM NODE ADJACENT TO REFLECTOR
412
IDENTIFY DOWNSTREAM NODE ADJACENT TO REFLECTOR
414
DESIGNATE NEXT REFLECTOR
416
GENERATE PROTECTION PATH FROM UPSTREAM NODE THROUGH NEXT REFLECTOR TO DOWNSTREAM NODE
NEXT REFLECTOR = SOURCE NODE?
418
NO
YES
END

FIG. 5


START
500
RESERVE WORKING BANDWIDTH FOR A CENTRAL NODE
502
DETERMINE WORKING BANDWIDTH FOR THE CENTRAL NODE BASED ON A PERIPHERAL NODE
504
DETERMINE PROTECTION BANDWIDTH FOR THE CENTRAL NODE BASED ON THE PERIPHERAL NODE
506
COMPARE WORKING BANDWIDTH FOR THE PERIPHERAL NODE TO PROTECTION BANDWIDTH FOR THE PERIPHERAL NODE
PROTECTION > WORKING?
508
NO
YES
RESERVE NO ADDITIONAL WORKING BANDWIDTH FOR THE CENTRAL NODE
512
RESERVE ADDITIONAL WORKING BANDWIDTH FOR THE CENTRAL NODE
510
MORE PERIPHERAL NODES?
514
YES
NO
END

IN ERNATIONAL SEARCH REPORT

International Application No
PCT/US 01/13732

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q11/04

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 99 11090 A (NORTHERN TELECOM LTD) 4 March 1999 (1999-03-04) page 4, line 25 -page 5, line 21	1,11,21
A	EP 0 959 641 A (CIT ALCATEL) 24 November 1999 (1999-11-24) abstract	1,11,21
A	TSONG-HO WU ET AL: "A PASSIVE PROTECTED SELF-HEALING MESH NETWORK ARCHITECTURE AND APPLICATIONS" IEEE / ACM TRANSACTIONS ON NETWORKING, IEEE INC. NEW YORK, US, vol. 2, no. 1, 1 February 1994 (1994-02-01), pages 40-52, XP000446089 ISSN: 1063-6692 abstract	1-27

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 October 2001	01 03 2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	STAESSEN, B

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 01/13732

B x I Observations where certain claims wer found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-27

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-27

A system, node and method for providing a protection path for connection-oriented signals in a telecommunications network.

2. Claims: 28-30

A method for reserving bandwidth for connection-oriented signals processed by a central node.

IN ERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 01/13732

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9911090 A	04-03-1999	WO 9911090 A1	04-03-1999
		EP 1010346 A1	21-06-2000
		JP 2001514478 T	11-09-2001
EP 0959641 A	24-11-1999	EP 0959641 A1	24-11-1999

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) Internati nal Publication Date
15 November 2001 (15.11.2001)

PCT

(10) International Publication Number
WO 01/86864 A3

(51) International Patent Classification[7]: H04Q 11/04

(21) International Application Number: PCT/US01/13732

(22) International Filing Date: 27 April 2001 (27.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/202,190	5 May 2000 (05.05.2000)	US
09/588,634	6 June 2000 (06.06.2000)	US

(71) Applicant: FUJITSU NETWORK COMMUNICATIONS, INC. [US/US]; 2801 Telecom Parkway, Mail Station 2C, Richardson, TX 75082 (US).

(72) Inventors: MO, Li; 4585 Spencer Drive, Plano, TX 75024 (US). WIDJAJA, Indra; 265 Avalon Gardens Drive, Nanuet, NY 10954 (US). SULLIVAN, Edward, T.; 417 Moran Drive, Highland Village, TX 75067 (US). WYNN, David, W.; 2614 Big Oaks Drive, Garland, TX 75044 (US).

(74) Agent: SHOWALTER, Barton, E.; Baker Botts L.L.P., 2001 Ross Avenue, Dallas, TX 75201-2980 (US).

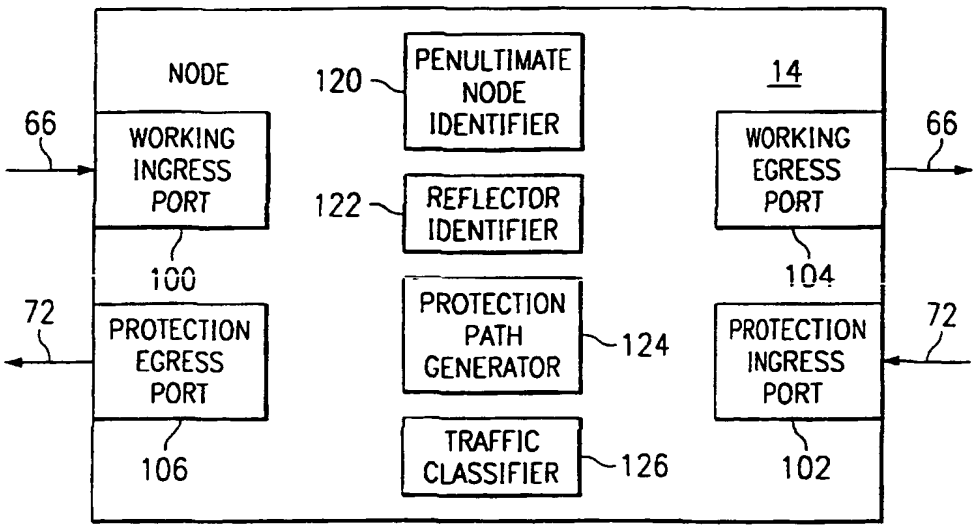
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR PROVIDING A PROTECTION PATH FOR CONNECTION-ORIENTED SIGNALS IN A TELECOMMUNICATIONS NETWORK



(57) Abstract: A system is provided for providing a protection path for connection-oriented signals in a telecommunications network comprising a plurality of nodes. The system includes a source node, a destination node and a penultimate node. The source node is operable to transmit traffic. The destination node is operable to receive traffic from the source node. The penultimate node is operable to receive traffic from the source node, to transmit traffic directly to the destination node, to designate one of the nodes as a reflector and to generate a first segment of a protection path from the penultimate node through the reflector to the destination node.

WO 01/86864 A3

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
25 April 2002

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.